# AES Notes
## Aaron Blumenfeld

AES has 10 rounds for 128 bits, 12 for 192 bits, 14 for 256 bits. Consider 128 bit AES. There are 4 steps: ByteSub (BS), ShiftRow (SR), MixColumn (MC), and AddRoundKey (ARK).

**Encryption:** ARK with 0th round key (which is the original key); nine rounds of BS, SR, MC, ARK with corresponding round keys; 10th round of BS, SR, ARK with 10th round key.

We have a 128-bit input, split into 16 bytes. Put them into a 4x4 matrix column by column. Each byte represents an element of $\mathbb{F}_{256} \simeq \mathbb{F}_2[x]/(x^8 + x^4 + x^3 + x + 1)$.

**ByteSub (BS):** There is an S-box. The first four bits of a byte tell you the row, and the last four tell you the column. BS gives you a new matrix, formed byte-by-byte using the output of the S-box.

**ShiftRow (SR):** Shift four rows cyclically to the right by 0, 1, 2, and 3.

**MixColumn (MC):** Given input matrix $M$, you get the output matrix $N$ with

$$N = \begin{pmatrix} x & x+1 & 1 & 1 \\ 1 & x & x+1 & 1 \\ 1 & 1 & x & x+1 \\ x+1 & 1 & 1 & x \end{pmatrix} M.$$

**AddRoundKey (ARK):** A round key is 128-bits. Put it into a 4x4 matrix of 16 bytes column-by-column and add (XOR) entry-by-entry (byte-by-byte) to the input matrix.

**Computing the Round Keys:** Put the original key into a 4x4 matrix (16 bytes). Expand the matrix by adding 40 more columns. Each column $i$ is called $W(i)$. The round key for round $i$ is the matrix with columns $W(4i), W(4i+1), W(4i+2), W(4i+3)$.

To define $W(4)$ through $W(43)$, we know $W(0)$ through $W(3)$, so define:

$$W(i) = \begin{cases} W(i-4) \oplus W(i-1) & \text{if } i \not\equiv 0 \pmod 4, \\ W(i-4) \oplus T(W(i-1)) & \text{if } i \equiv 0 \pmod 4. \end{cases}$$

Now to form $T(W(i-1))$, let $W(i) = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$. Then shift $W(i)$ up cyclically to form $\begin{pmatrix} b \\ c \\ d \\ a \end{pmatrix}$. Replace each byte in this column vector with the corresponding bytes in the S-box from BS to get $\begin{pmatrix} e \\ f \\ g \\ h \end{pmatrix}$. Compute the round constant $r(i) = x^{(i-4)/4}$. Then

$$T(W(i-1)) = \begin{pmatrix} e \oplus r(i) \\ f \\ g \\ h \end{pmatrix}.$$

**Decryption:** ARK with 10th round key; nine rounds of inverse BS, inverse SR, inverse MC, inverse ARK with round keys 9 to 1; inverse BS, inverse SR, ARK with 0th round key.